## REMARKS

This Amendment is in response to the Office Action mailed June 28, 2006. Claims 1-4, 8-18 and 21-32 are pending in this case. Claims 1-4, 8-18 and 21-32 have been rejected. Claims 1, 3, 4, 8, 9, 10, 12, 14, 15, 16 and 30 have herein been amended. Claims 25 and 28 have herein been canceled. Claims 2, 11, 13, 17-18, 21-24, 26-27, 29 and 31-32 remain unchanged.

Claims 1-2, 4, 9-10, 12-14 and 16 have been rejected under 35 U.S.C. 102(b) as being anticipated by Cordery et al. (US 6,073,125). For the following reasons, the 102(b) rejection is respectfully traversed.

Cordery et al. does not disclose the same steps as Claims 1-2, 4, 9-10, 12-14 and 16, and thus does not anticipate Claims 1-2, 4, 9-10, 12-14 and 16 under the law pertaining to 35 U.S.C. §102 ("identity of invention"). Cordery et al., unlike Applicants' method for providing traceability of mail pieces, relates to a "*mail payment and evidencing systems and, more particularly, to a token key distribution system for mail payment and evidencing system.*" (See Col. 1, lines 6-9). In other words, Cordery et al. relates to mail payment systems, and is concerned with verifying payment and preventing counterfeit postage. (See Col. 2, lines 58-62: "*Digital tokens provide a basis for verifying payment for an indicium through use of a secret key [$K_m$]...*"). Clearly, Cordery et al. is not concerned with source identification of mail pieces for mail security and traceability, as in Applicants' claimed embodiments.

Cordery et al. relates to mail payment (accounting) verification systems, and specifically verification of encrypted mailpiece indicia generated by a meter using a random digital token key $K_m$ (See Abstract). The digital token key $K_m$ used in Cordery et al. is not a source tracing code corresponding to a source of the mailpiece, used for source tracing purposes. In Cordery et al., a secure device (vault) 114 generates a random digital token key $K_m$, which is used to imprint mailpieces with

encrypted indicia (See Column 3, lines 30-32; Column 4, lines 20-21; and Column 6, lines 11-14). Next, a statement of mail is prepared, which includes the random digital token key $K_m$ encrypted with an acceptance unit key ($P_{AU}$) (See Column 3, lines 32-36; Column 5, lines 20-24; and Column 6, lines 17-18[1]).

The mailpieces and the statement of mail are then brought to a mail acceptance unit or mail authentication unit. To verify the encrypted mailpiece indicia for payment (accounting) purposes, the authentication unit decrypts the encrypted random digital token key $K_m$ from the statement of mail using the private key $P'_{AU}$, and then verifies the mailpiece indicia with the digital token key $K_m$ (See Column 3, lines 44-46; Column 5, lines 28-32; and Column 6, lines 38-42).

Cordery et al. also discloses a statement of mail signature confirmation process. The meter which generates the encrypted mailpiece indicia has a meter identification number (MID). A pair of meter keys $P_{MID}$ (public) and $P'_{MID}$ (private) corresponding to that meter are provided to the secure device (vault), with the public meter key $P_{MID}$ being provided to each acceptance unit (See Column 3, lines 12-21). The secure device (vault) signs the statement of mail using the private meter key $P'_{MID}$. To verify this signature, the acceptance unit uses the MID from the statement of mail as a pointer to look-up the public meter key $P_{MID}$ in its database in order to verify the $P'_{MID}$ signature (See Column 3, lines 36-42; and Column 6, lines 21-39[2]). It is noted that this signature verification occurs prior to and separate from the mailpiece indicia verification process using the digital token key $K_m$, discussed above (See Column 6, lines 36-41). It is also noted that the meter keys are associated with the statement of

---

1 In Column 6, line 17, the public key $P_{AU}$ is erroneously referred to as "$P'_{AU}$" (which is the symbol for the private key).

2 In Column 6, line 39, the public meter key $P_{MID}$ is erroneously referred to as "$P'_{MID}$" (which is the symbol for the private meter key).

mail only, to verify the signature. Cordery et al. does not disclose use of either of the meter keys $P_{MID}$ and $P'_{MID}$ on the mailpieces or to verify source or trace the mailpieces to a source.

Accordingly, it should be readily apparent that Cordery et al.'s method of verifying payment for mailpiece indicia is very different from and clearly does not anticipate (or make obvious) Applicants' claimed methods for providing traceability of mailpieces. Specifically, with respect to amended Claim 1, Cordery et al. fails to anticipate a method for providing traceability of mailpieces, and the claimed steps of providing a first source tracing code on each of said plurality of mail pieces, said first source tracing code corresponding to a source of the mail pieces; providing a second source tracing code on said mailing statement, said second source tracing code corresponding to said source of the mail pieces; and verifying that said first source tracing code corresponds to said second source tracing code, wherein verified mailpieces can be traced back to the source of the mailpieces by reading the first source tracing code.

Contrary to the assertion in the rejection, Cordery et al.'s encrypted indicia do not anticipate a first source tracing code corresponding to the source of the mailpieces. Cordery et al.'s encrypted indicia are simply traditional indicia encrypted with the random digital token key $K_m$. The key $K_m$ is nothing more than a randomly changing key (See Column 2, lines 20-22). Thus, the key $K_m$ does not correspond to anything. It is random and does not correspond to the source of the mailpieces. Further, meter imprints or indicia do not identify the mailer using that meter. At most, it will only identify the manufacture of the meter.

Similarly, Cordery et al.'s encrypted random digital token key $K_m$ on the statement of mail, i.e., $(K_m)\ P_{AU}$ (see reference 312, Figure 3) does not anticipate a second source tracing code corresponding to the source of the mailpieces. Cordery et al.'s encrypted random digital token key $K_m$ 312 is simply the

random key $K_m$ encrypted with the acceptance unit public key $P_{AU}$. Again, the random key $K_m$ does not correspond to anything. The acceptance unit key $P_{AU}$ is simply used for encryption on the statement of mail, and at most corresponds to the specific acceptance/authentication unit (see Column 4, 48-56). Thus, neither ($K_m$) nor $P_{AU}$ (nor the combination of the two, i.e., encrypted key $K_m$ 312) corresponds to the source of the mailpieces.

In Cordery et al., the authentication/acceptance unit uses the digital token key $K_m$ which was decrypted from the statement of mail to verify the encrypted indicia of the mailpieces (see Column 6, lines 39-42) in order to detect counterfeit indicias (see Column 2, lines 58-67). As such, there is no verification of any source tracing codes in Cordery et al. It can thus be seen that Cordery et al.'s verified mailpieces cannot be traced back to the source of the mailpieces by reading the random digital token key $K_m$.

Once again, the random digital token key $K_m$ does not correspond to anything – it is random. The rejection, p. 3, asserts that the key $K_m$ relates to various information including origin postal code... (citing Fig. 2 and Column 4, lines 42-58). This assertion is inaccurate. As discussed in Column 4, lines 42-58, it is the non-volatile memory 210 which stores this various information. This various information stored in the non-volatile memory 210 is used to generate or is "related to generating" the encrypted indicia and digital token (i.e., the specific meter marking or amount of digital postage, encrypted with the random digital token). However, it remains clear that the encrypted indicia with random digital token $K_m$ does not correspond to a source of the mailpieces, such that the mailpieces can be traced back to the source by reading the random digital token. Nonetheless, the origin postal code (i.e., zip code) does not correspond to the source, only at most to a general location (e.g., city).

For the above reasons, Cordery et al. does not anticipate Claim 1. It is noted that while the European Patent Office applied Cordery et al. in rejecting the claims in Applicants' related European Patent Application, a different set of claims was involved in the European Patent Application, and as such, the European Patent Office's reasoning is inapplicable to the claims pending in this Application. Further, it is apparent that the European Patent Office did not contemplate or consider the specific remarks and arguments set forth herein with respect to Cordery et al., which clearly identify and discuss key distinctions and differentiations between Cordery et al. and the claims pending in this Application. The remarks and arguments herein definitively traverse the European Patent Office's interpretation of Cordery et al.

With respect to Claim 2, for the reasons discussed above, there are no corresponding first tracing code and/or second tracing code in Cordery et al. The random digital token $K_m$ simply does not correspond in any way to a source of the mailpieces. Further, as discussed above, Cordery et al. step of verifying is for verifying postage, unlike Applicants' step of verifying which allows verified mailpieces to be traced back to the source of the mailpieces. As such, Cordery et al. does not anticipate Claim 2.

With respect to Claims 4, 9 and 10, as discussed above, Cordery et al.'s random digital token $K_m$ (which is not a tracing code) is produced by a meter and is part of a meter imprint or indicium. As such, the random digital token $K_m$ is not embedded into a digital image, a text, a watermark, paper fibers or invisible ink (as in amended Claim 4), as opposed to meter imprint; is not produced by passing the mailpieces through tracing code producing equipment (as in amended Claim 9), as opposed to a meter; and is not independent from a meter imprint, digital postage mark or indicia (as in Claim 10).

Further with respect to Claim 9, the rejection, p. 3, cites to Cordery et al., Figure 2 and Column 2, lines 40+, in an attempt to equate Cordery et al.'s vault 114 to Applicant's tracing code producing

equipment. However, Cordery et al.'s vault 114 merely generates the random digital token key $K_m$, it does not produce the encrypted indicia on the mailpieces. Instead, the meter imprints the encrypted indicia on the mailpieces in Cordery et al. Thus, the mailpieces in Cordery et al. are not passed through tracing code producing equipment. They are simply passed through the meter associated with the vault. Clearly, there are no source tracing codes and there is no source tracing code producing equipment disclosed in Cordery et al.

Further with respect to Claim 10, the rejection, p. 3, also suggests that Cordery et al.'s *"first tracing code is independent from a meter imprint (i.e., the first tracing code is encrypted with a random digital token key)."* This is inaccurate. In the rejection, p. 3, the random digital token key $K_m$ is alleged to be the first tracing code (they are one and the same). Key $K_m$ is random. It is not encrypted on the mailpiece. Key $K_m$ is encrypted on the statement of mailing with acceptance unit key $P_{AU}$, but that is not the first tracing code which is on the mailpieces.

With respect to Claims 12 and 13, for the reasons discussed above with respect to Claims 1, 9 and 10, Cordery et al. does not anticipate Claims 12 and 13.

With respect to Claim 14, for the reasons discussed above with respect to Claim 4, Cordery et al. does not anticipate Claim 14.

With respect to Claim 16, for the reasons discussed above with respect to Claim 10, Cordery et al. does not anticipate Claim 16.

Accordingly, Cordery et al. clearly does not anticipate Applicants' Claims 1-2, 4, 9-10, 12-14 and 16 under the law pertaining to 35 U.S.C. 102(b). Applicants respectfully assert that Claims 1-2, 4, 9-10, 12-14 and 16 are allowable over Cordery et al. An early notice of allowance is respectfully requested.

Claim 3 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Cordery et al. in view of Clark et al. (US 4,829,568). For the following reasons, the Examiner's rejection is respectfully traversed.

The proposed combination does not make obvious Applicants' Claim 3. Clark et al. fails to make up for the above identified deficiencies of Cordery et al. As such, the proposed combination of Cordery et al. in view of Clark et al. fails to teach, suggest or disclose the method claimed in Applicant's Claim 3. Additionally, Clark et al. relates to a system for the metering of encrypted postage and similar indicia to inhibit forgery and alteration of the same (see Abstract). The data provided in the indicia is the typical indicia data such as the postage fee, the date, the sending station [meter] serial number [meter ID number], the zip code, mail piece count and weight (see Column 3, lines 9-13; Column 6, lines 37-40; Column 13, lines 5-12, 25-37 and 47-53). As previously indicated with respect Cordery et al., this traditional data in meter imprints or indicia does not identify the mailer using that meter. At most, it will only identify the manufacture of the meter and the zip code location of the mailer. Nonetheless, Claim 3 has been amended to indicate that Applicants' first source tracing code is independent of the meter imprint, digital postage mark or postal indicia. Neither reference in the proposed combination is independent of the meter indicia in this regard.

Accordingly, Cordery et al. in view of Clark et al. does not make obvious Applicants' Claim 3 under the law pertaining to 35 U.S.C. 103. Applicants respectfully assert that amended Claim 3 is allowable over the proposed combination. An early notice of allowance is respectfully requested.

Claims 8, 15, 18, 21-25, 27-28 and 30-31 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Cordery et al. in view of Simon (US 20030085266). For the following reasons, the Examiner's rejection is respectfully traversed.

The proposed combination does not make obvious Applicants' Claims 8, 15, 18, 21-25, 27-28 and 30-31. Simon fails to make up for the above identified deficiencies Cordery et al. As such, the proposed combination of Cordery et al. in view of Simon fails to teach, suggest or disclose Applicants' claimed method(s). Further, Cordery et al. relates to a postage verification system, while Simon relates to a safety apparatus for postal services. The respective subject matter in these references is unrelated. As such, there is no motivation or suggestion in either reference for their combination.

Further, in addition to the above described deficiencies of Cordery et al., Cordery et al. admittedly does not disclose the step of capturing an identity of an individual submitting the mail piece(s). Simon is being cited to show a mail-collection receptacle (mailbox) equipped with a receiver 3, which allegedly captures an image of the mail piece and the face of a person making the deposit. Even if these references are combined, the combination fails to make obvious the rejected claims.

Simon's apparatus does nothing more than *attempt* to capture an image of a person depositing a mail piece into a mailbox and at the same time an image of the mail piece itself, and then stores the captured images. However, there is never any source tracing code on the mail pieces. There is nothing on the mail pieces to read and trace back to any source. Instead, a particular mail piece of interest (or its image) would have to be randomly compared to the captured image of all of the stored mail pieces images (which could be millions and millions) in order to try to find a match. This could prove impossible, especially if the mail piece was deposited within a stack of mail pieces, or if it was deposited upside down. In these cases, no image of that mail piece could be recorded. Further, the person depositing the mail would have to be directly in front of the camera for image capture, and if standing to the side of the mailbox, no image of that person would be captured. Still further, conventional surveillance cameras as may be used in Simon are typically of mediocre quality at best, and any captured

images are typically lacking definition, detail and/or clarity. Thus, even if there was motivation to combine Simon with Cordery et al., the combination not only still fails to make obvious all of Applicants' claim limitations, but also would not result in a system which could not perform the claimed steps of Applicants' claims.

Specifically, with respect to amended Claim 8 and Claim 24, for the reasons discussed above with respect to Claim 1, Cordery et al. and thus the proposed combination fails to teach or disclose any source tracing codes on the mail pieces and statement of mail. Further, Simon and thus the proposed combination fails to teach or disclose storing any first or second source tracing code in association with the recorded identity of the individual. Additionally, the proposed combination fails to teach, suggest or disclose the step of subsequently using the first or second source tracing code to trace at least one of the plurality of mail pieces back to at least one of the individual submitting the mail pieces and the source of the mail pieces.

With respect to amended Claim 15 and Claim 27, for the reasons discussed above with respect to Claims 12 and 8, the proposed combination fails to suggest or disclose Claim 15.

Independent Claim 18 and Claims 21- 23 are free from the applied art for the reasons discussed above with respect to Claims 8 and 12. Moreover, independent claim 18 describes a method for providing traceability of mail pieces including the pertinent steps of providing a source tracing code on the at least one mail piece via source tracing code producing equipment after the at least one mail piece has been submitted to the postal facility; and storing information produced by the source tracing code producing equipment in association with the captured and stored identity of the individual submitting the at least one mail piece. The Examiner's proposed combination of references fails to make obvious the steps of providing a source tracing code on the at least one mail piece via source tracing code producing

equipment after the at least one mail piece has been submitted to the postal facility; and storing information produced by the source tracing code producing equipment in association with the captured and stored identity of the individual submitting the at least one mail piece.

With respect to Claims 30 and 31, in addition to the reasons discussed above with respect to Claims 8 and 12, the proposed combination fails to make obvious the steps of providing an encrypted tracing code on at least one envelope; subsequently providing the at least one envelope having the encrypted tracing code to a mailer to produce at least one mail piece; recording the identity of the mailer in association with the encrypted tracing code; and reading the encrypted tracing code on the at least one mail piece to verify the source of the mail piece. By providing the encrypted tracing code on an envelope prior to providing the envelope to the mailer for the production of the mail piece, individuals or businesses can obtain secure, personalized envelopes as discussed for example starting at line 17 of page 10 of the present Application. This is not contemplated or suggested by the proposed combination of references.

Accordingly, the combination of Cordery et al. in view of Simon does not make obvious Applicants' Claims 8, 15, 18, 21-25, 27-28 and 30-31 under the law pertaining to 35 U.S.C. 103. Applicants respectfully assert that Claims 8, 15, 18, 21-24, 27 and 30-31 are allowable over the proposed combination. An early notice of allowance is respectfully requested.

Claims 11, 17, 26, 29 and 32 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Cordery et al. in view of Simon and further in view of Pintsov (US 6,009,416). For the following reasons, the Examiner's rejection is respectfully traversed.

The proposed combination does not make obvious Applicants' Claims 11, 17, 26, 29 and 32. Pintsov fails to make up for the above identified deficiencies of Cordery et al. in view of Simon. As

such, the proposed combination of Cordery et al. in view of Simon and further in view of Pintsov fails to teach, suggest or disclose Applicants' claimed method(s).

Further, in addition to the above described deficiencies of Cordery et al. in view of Simon, that combination admittedly does not disclose the step of providing an alert indication when the first and second codes do not correspond. Pintsov is being cited to teach that *"a suitable investigation can be implemented when information obtained from a scanned mail piece does not match with the corresponding statement of mail."* However, implementing a suitable investigation does not equate to or require providing an alarm indication, and as such, Pintsov does not disclose or suggest providing an alarm indication. The suitable investigation could take place in the absence of an alarm indication. Therefore, even if combined, the combination of Cordery et al. in view of Simon and further in view of Pintsov fails to make obvious Claims 11 and 17.

With respect to Claims 26, 29 and 32, the proposed combination of Cordery et al. in view of Simon and further in view of Pintsov fails to teach, suggest or disclose tracing a source tracing code back to the source of the mail pieces, to determine a reason why the codes do not correspond. There is nothing in Pintsov, and thus the proposed combination, to suggest that the suitable investigation includes tracing a code back to the source to determine a reason as to why the codes do not correspond. Instead, it is likely that the suitable investigation in Pintsov would simply require and internal review of the mail pieces and the mailing statement and nothing more.

Accordingly, Cordery et al. in view of Simon and further in view of Pintsov does not make obvious Applicants' Claims 11, 17, 26, 29 and 32 under the law pertaining to 35 U.S.C. 103. Applicants respectfully assert that Claims 11, 17, 26, 29 and 32 are allowable over the proposed combination. An early notice of allowance is respectfully requested.

It is respectfully submitted that none of the prior art of record, either alone or in combination, fairly teaches, suggests or discloses the novel and unobvious features of Applicants' claims as set forth herein. Accordingly, Applicants respectfully assert that all of the claims as presented herein are now in condition for immediate allowance. An early notice allowance is respectfully requested.

Any arguments of the Examiner not specifically addressed should not be deemed admitted, conceded, waived, or acquiesced by Applicants. Any additional or outstanding matters the Examiner may have are respectfully requested to be disposed of by telephoning the undersigned.

A supplemental Information Disclosure Statement is enclosed.

A petition for a one month extension of time is enclosed.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Brian K. Seidleck
Registration No. 51,321

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 BKS:idw
Facsimile: 202.756.8087
**Date: October 26, 2006**

**Please recognize our Customer No. 20277 as our correspondence address.**